

DAVID Y. IGE
GOVERNOR

JOSH GREEN
LT. GOVERNOR

**STATE OF HAWAII
OFFICE OF THE DIRECTOR
DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS**

335 MERCHANT STREET, ROOM 310

P.O. BOX 541

HONOLULU, HAWAII 96809

Phone Number: 586-2850

Fax Number: 586-2856

cca.hawaii.gov

CATHERINE P. AWAKUNI COLÓN
DIRECTOR

JO ANN M. UCHIDA TAKEUCHI
DEPUTY DIRECTOR

Testimony of the Department of Commerce and Consumer Affairs

**Before the
Senate Committee on Commerce, Consumer Protection, and Health
and
Senate Committee on Technology**

**Tuesday, March 17, 2020
9:00 am
State Capitol, Conference Room 229**

**On the following measure:
H.B. 2572, H.D. 2, RELATING TO PRIVACY**

Chair Baker, Chair Keohokalole, and Members of the Committees:

My name is Stephen Levins, and I am the Executive Director of the Department of Commerce and Consumer Affairs' (Department) Office of Consumer Protection (OCP). The Department appreciates the intent of and offers comments on this bill.

The purposes of this bill are to: (1) modernize "personal information" for the purposes of security breach of personal information law; (2) prohibit the sale of geolocation information and internet browser without consent; (3) amend provisions relating to electronic eavesdropping law; and (4) prohibit certain manipulated images of individuals.

The Department supports H.D. 2's expansion of the definition "personal information" in Hawaii Revised Statutes (HRS) chapter 487N because the current definition is obsolete. Businesses that collect or store data digitally have a responsibility

to protect information that is sensitive, confidential, or identifiable from access by hackers; these businesses also have a responsibility to prevent the data from being made available to criminals who engage in identity theft. As of 2018, all 50 states have data breach notification laws that prescribe when consumers must be notified when their “personal information” has been breached. Hawaii’s data breach notification laws were codified in 2006 as HRS chapter 487N, which, in pertinent part, defines “personal information” in relation to when a breach notification is required, and specifies the circumstances in which a business or government agency must notify a consumer that his or her personal information has been breached. Although Hawaii was one of the first states to enact this law, advancements in technology have made identity theft easier than it was 14 years ago. Businesses and government agencies now collect far more information, and bad actors exploit vulnerabilities in computer databases for nefarious purposes and with increased frequency.

H.D. 2 corrects existing statutory inadequacies by expanding the definition of “personal information” to include various personal identifiers and data elements, such as email addresses, health insurance policy numbers, security codes, and medical histories. This will enhance consumer protections involving privacy and align with legislation recently enacted in other jurisdictions, including Vermont and California.

With respect to the other elements of H.D. 2, the Department believes that the bill’s regulation of geolocation data and internet browser information as set forth in part III will advance consumer privacy by prohibiting the sale of consumers’ location data and browsing history without their consent. Lastly, the Department takes no position regarding parts IV and V, since they primarily impact criminal enforcement.

Thank you for the opportunity to testify on this bill.



**TESTIMONY BEFORE THE SENATE COMMITTEES ON
COMMERCE, CONSUMER PROTECTION, AND HEALTH
&
TECHNOLOGY**

H.B. 2572, HD2

Relating to Privacy

Tuesday, March 17, 2020

9:00 a.m.

State Capitol, Conference Room 229

Wendee Hilderbrand
Managing Counsel & Privacy Officer
Hawaiian Electric Company, Inc.

Dear Chair Baker and Chair Keohokalole, Vice Chair Chang and Vice Chair English and Members of the Committees,

My name is Wendee Hilderbrand, and I am testifying on behalf of Hawaiian Electric Company, Inc. (Hawaiian Electric) **with comments on and suggested amendments to H.B. 2572, HD2**. While Hawaiian Electric is supportive of modernizing Hawaii's data breach statute, several of the provisions in Part II of the proposed legislation go further than the vast majority of other state data security statutes and would lead to significant unintended compliance consequences.

Part II of the bill is intended to update Hawaii's data breach notification statutes, H.R.S. § 487N-1 *et seq.*, by including additional types of data in the definition of "Personal Information," and thereby, expanding the scope of what constitutes a "security breach." Importantly, H.R.S. § 487N-2, like most state data breach notification statutes, has one primary objective: to protect individuals against

identity theft by requiring that they receive notification if certain types of their data (e.g., social security numbers, drivers' license numbers) are compromised, so they can take steps to protect themselves (e.g., credit monitoring, credit freeze).

Part II of H.B. 2572, HD2, proposes to add health information to the definition of "Personal Information" in H.R.S. § 487N-1. See H.B. 2572, HD2, Part II, § 2(1)(7). While we agree that health information should be kept confidential and secure, it is not the type of information that subjects individuals to the risk of identity theft, and thus, is ill-suited for H.R.S. § 487N-1. Rather, the confidentiality and security of health information is better addressed by the Health Insurance Portability and Accountability Act ("HIPAA"). HIPAA and its enacting regulations are among the most protective privacy laws in the world; however, they also address considerations unique to health information, such as the business use exception, risk of harm analysis, and implicit consent.

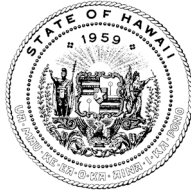
Some of the unintended consequences that could arise if health information is added to H.R.S. § 487N-1 include prohibitions on internal "safety alerts" that advise of workplace injuries as a teaching tool; difficulty in investigating medical leave abuses; impediments to employer-sponsored flu shot or blood drives; prohibitions on workplace wellness challenges or weight loss competitions; and bans on interoffice emails advising of a family illness or birth of a baby. Health information is not related to identity theft, is heavily regulated by HIPAA, and should not be in Hawaii's data breach notification statutes.

Finally, Hawaiian Electric has concerns that Part II of the legislation attempts to expand protection of passwords in a way no other jurisdiction has done, without explanation or reason. Currently, H.R.S. § 487N-1 protects financial account

numbers, as well as passwords that “would permit access to an individual’s financial account.” *Id.* at (3) (emphasis added). H.B. 2572, HD2 separates account numbers and passwords into two subparagraphs, each with expanded language, but only includes the important qualifying word “financial” in the subparagraph relating to account numbers, inexplicably omitting it from the subparagraph relating to passwords. *Compare id.* at Part II, § 2(1)(4) with § 2(1)(5). This seemingly small omission would result in unprecedented protection of all passwords regardless of what the passcode is connected to (e.g., a Netflix or Snapfish account) or whether it poses any danger of identity theft. No other statute has included such broad protection of passwords, and there is no explanation in the Twenty-First Century Privacy Law Task Force Report as to why the qualifying word “financial” was or should be removed from the subparagraph relating to passwords.

Accordingly, Hawaiian Electric respectfully requests that H.B. 2572, HD2, Part II, Section 2 be amended by deleting subparagraph (7) regarding health care and adding the word “financial” to subparagraph (5) (i.e., password that would allow access to an individual’s financial account;”). Thank you for this opportunity to testify.

DAVID Y. IGE
GOVERNOR



DOUGLAS MURDOCK
CHIEF INFORMATION
OFFICER

OFFICE OF ENTERPRISE TECHNOLOGY SERVICES

P.O. BOX 119, HONOLULU, HI 96810-0119
Ph: (808) 586-6000 | Fax: (808) 586-1922
ETS.HAWAII.GOV

Testimony of
DOUGLAS MURDOCK
Chief Information Officer
Enterprise Technology Services

Before the

SENATE COMMITTEE ON COMMERCE, CONSUMER PROTECTION, AND HEALTH
SENATE COMMITTEE ON TECHNOLOGY
TUESDAY, MARCH 17, 2020

HOUSE BILL NO. 2572 HD2
RELATING TO PRIVACY

Dear Chairs Baker and Keohokalole, Vice Chairs Chang and English, and members of the committee:

The Office of Enterprise Technology Services (ETS) supports HB 2572 HD2, which redefines "personal information" for the purposes of security breach of personal information law, establishes new provisions on consumer rights to personal information and data brokers, prohibits the sale of geolocation information and internet browser information without consent, amends provisions relating to electronic eavesdropping law, prohibits certain manipulated images of individuals.

As chair of the Information Privacy and Security Committee created under HRS Section 487N, we support updating the definition of "personal information" in HRS Section 487N that includes expanded identifiers and data elements which are consistent with prevailing practices for current security breach notification laws.

Thank you for the opportunity to provide testimony on this measure.



March 17, 2020

Committee on Technology
Sen. Keohokalole Chair
Sen. English, Vice Chair

Committee on Consumer
Protection and Health
Sen. Baker, Chair
Sen. Chang, Vice Chair

The Senate
The Thirtieth Legislature
Regular Session of 2020

RE: HB 2572, HD2- RELATING TO PRIVACY
DATE: Tuesday, March 17, 2020
TIME: 9:00am
PLACE: Conference Room 229
State Capitol 415 South Beretania Street, Honolulu HI

Aloha Chairs Keohokalole and Baker, Vice Chairs English and Chang, and the Members of the Committees,

Thank you for the opportunity to testify in **support** of **part V of HB2572 HD2** found on page 20 of the measure.

[SAG-AFTRA](#) represents over 1100 actors, recording artists, and media professionals in our state. We are the professional performers working in front of the camera and behind the microphone. We work in an industry that has seen tremendous advancement in the technology used to create and disseminate content. This evolution in content creation and distribution has not only led to an exponential growth in production and consumption of content, it has equalized the means of creation, broken down the barriers to entry and allowed for professional looking content created by almost anyone with determination and a smart phone.

However, there is a dark side to all this advancement. This dark side can be summed up by a new word that has entered our lexicon: Deepfakes. The same technology used to create younger versions of actors in movies, or insert actors who are no longer able to perform in movies due to death or unavailability, can now be used to create realistic non-consensual pornographic digital content. New technologies allow content creators to manipulate images to depict individuals as engaging in sexual activity or as performing in the nude without their consent or participation. Specifically, Internet users can use a publicly available artificial intelligence algorithm to transform still images of a person into live action performance by realistically inserting their face onto the body of a porn performer.

A recent Washington Post article, accessed [here](#), describes how “Fake-porn videos are being weaponized to harass and humiliate women: ‘Everybody is a potential target.’” Just as a smart phone has turned all of us into filmmakers with free and easily accessible distribution avenues (TikTok, Facebook, Instagram etc...), the same technology can be used to violate privacy, harass and abuse, turning unwilling people (mostly women) into porn stars.

Mericia Palma Elmore, Executive Director
SAG-AFTRA Hawaii Local
mericia.palmaelmore@sagaftra.org
Ph: 808-596-0388 • Fax: 808-593-2636
201 Merchant St Suite 2301 Honolulu, HI 96813

SCREEN ACTORS GUILD - AMERICAN FEDERATION OF
TELEVISION AND RADIO ARTISTS
SAGAFTRA.org
Associated Actors & Artistes of America / AFL-CIO

This proposed legislation amends HRS 711-1110.9 to include nonconsensual, digitally produced sexually explicit material, such as Deepfakes pornography, among the offences that constitute a violation of privacy in the first degree.

This amendment to HRS 711-1110.9 not only fits squarely within Hawaii's revenge porn laws, it also fulfills the constitutional mandate set forth in Section 6 of the Hawaii Constitution, requiring the legislature to take affirmative steps to implement rules that guarantee that the people's right to privacy be recognized and shall not be infringed.

We respectfully urge you to pass this section to protect not only our professional performers from exploitation, but to protect our daughters, sisters and mothers from this abusive violation privacy.

Thank you again for your continued support and please don't hesitate to contact the SAG-AFTRA Hawaii Local office for more information on this issue as it relates to professional performers.

Respectfully,



Mericia Palma Elmore
Executive Director SAG-AFTRA Hawaii Local

**SENATE COMMITTEES ON
JUDICIARY AND COMMERCE, CONSUMER PROTECTION, and HEALTH AND
TECHNOLOGY**

March 17, 2020

House Bill 2572 HD2 Relating to Privacy

Chair Baker, Vice-Chair Chang, Chair Keohokalole, Vice-Chair English, and members of the Senate Committees on Commerce, Consumer Protection and Health, Technology, I am Rick Tsujimura, representing State Farm Mutual Automobile Insurance Company (State Farm). State Farm offers these comments about [HB2572 HD2](#) Relating to Privacy.

State Farm understands and shares the Legislature's concern for protecting the privacy of information that consumers give to businesses to allow the businesses to provide the products and services that consumers desire. There are numerous Federal and State laws that provide such protections. With that in mind, below are some specific comments and suggested amendments:

1. P. 5, *ll.* 4-5, defining a social security as a "specified data element." A normal practice to mask a social security number is to truncate it to include only the last four digits. State Farm recommends striking the following: "~~either in its entirety or the last four or more digits~~".
2. P. 9, *l.* 21 through P. 10, *l.* 4. These lines follow the definition of "sale" in the portion dealing with the sale of "geolocation information," and specifically state what *is not* considered to be a sale under the provision. There are situations where a company has a legitimate need to share this information with an affiliated company or a service provider in order to provide necessary services to a customer, or transfer the information as part of a merger or transfer of part of or part of a business. For this reason, State Farm recommends amending this provision beginning a P. 9, *l.* 21 so it reads as follows:

"Sale" shall not include the releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a user's geolocation information

(1) ~~f~~For the purpose of responding to an emergency;

(2) To an affiliate company, or to a third party service provider;

(3) As part of a proposed or actual sale, merger transfer, or exchange of all or a portion of the business or an operating unit of the business.

3. P. 11, *l.* 16. Unlike the definitions for "geolocation information," those for "internet browser information" do not state what *is not* considered to be a sale under the provision.

Similar to “geolocation information,” there are situations where a company has a legitimate need to share internet browser information with an affiliated company or a service provider in order to provide necessary services to a customer, or transfer the information as part of a merger or transfer of part of or part of a business. For this reason, State Farm recommends amending this provision beginning adding the following beginning at P. 11, l. 16, to read as follows:

“Sale” shall not include the releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a user’s internet browser information

(1) To an affiliate company, or to a third party service provider;

(2) As part of a proposed or actual sale, merger transfer, or exchange of all or a portion of the business or an operating unit of the business.

Thank you for considering these comments and suggestions.

HAWAII FINANCIAL SERVICES ASSOCIATION

c/o Marvin S.C. Dang, Attorney-at-Law

P.O. Box 4109

Honolulu, Hawaii 96812-4109

Telephone No.: (808) 521-8521

March 17, 2020

Senator Rosalyn H. Baker, Chair, and Senator Stanley Chang, Vice Chair,
and members of the Senate Committee on Commerce, Consumer Protection, and Health
Senator Jarrett Keohokalole, Chair, and Senator J. Kalani English, Vice Chair,
and members of the Senate Committee on Technology
Hawaii State Capitol
Honolulu, Hawaii 96813

Re: **H.B. 2572, H.D. 2 (Privacy)**
Hearing Date/Time: Tuesday, March 17, 2020, 9:00 p.m.

I am Marvin Dang, the attorney for the **Hawaii Financial Services Association** (“HFSA”). The HFSA is a trade association for Hawaii’s consumer credit industry. Its members include Hawaii financial services loan companies (which make mortgage loans and other loans, and which are regulated by the Hawaii Commissioner of Financial Institutions), mortgage lenders, and financial institutions.

The HFSA offers comments and a proposed amendment.

This Bill does the following: (1) modernizes "personal information" for the purposes of security breach of personal information law, (2) prohibits the sale of geolocation information and internet browser information without consent, (3) amends provisions relating to electronic eavesdropping law, and (4) prohibits certain manipulated images of individuals.

On page 5, lines 3-16, is the following definition which would amend Hawaii’s existing law regarding security breach of personal information:

“Specified data element” means any of the following:

- (1) An individual's social security number, either in its entirety or the last four or more digits;
- (2) Driver's license number, federal or state identification card number, or passport number;
- (3) A federal individual taxpayer identification number;
- (4) An individual's financial account number or credit or debit card number;
- (5) A security code, access code, personal identification number, or password that would allow access to an individual's account;
- (6) Health insurance policy number, subscriber identification number, or any other unique number used by a health insurer to identify a person;

...

We agree that if an individual’s entire social security number (i.e. the entire 9 digits) is displayed, that should be included in the “specified data element” definition. This would be similar to the other portions of the proposed “specified data element” definition, e.g. displaying the entire driver’s license number, the entire federal taxpayer identification number, the entire financial account number, etc.

However, this Bill would unnecessarily go further: it would include as a “specified data element” the “last four or more digits” of the 9 digit social security number. In other words, the social security number would not be a “specified data element” only if the number was shortened down to xxx-xx-x321.

We are unaware of a similar statutory restriction in any state. In fact, the standard and usual practice in the United States is to allow shortening, truncating, abbreviating, or limiting the display of an individual’s

social security number down to the last 4 digits, e.g. xxx-xx-4321. That's the practice for Hawaii financial industry, Hawaii courts, and others.

For that reason, we respectfully contend that only when more than the last 4 digits is shown, it should be a "specified data element" for the purpose of the law for security breach of personal information. For example, displaying xxx-x5-4321 would be a "specified data element, but displaying xxx-xx-4321 would not be.

Accordingly, here's our two alternate proposed amendments:

PROPOSED AMENDMENT #1:

"Specified data element" means any of the following:

- (1) An individual's social security number, either in its entirety or the last four or more digits];

...

OR

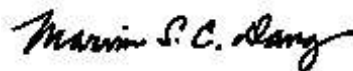
PROPOSED AMENDMENT #2:

"Specified data element" means any of the following:

- (1) An individual's social security number, either in its entirety or **more than** the last four **or more** digits;

...

Thank you for considering our testimony.



MARVIN S.C. DANG
Attorney for Hawaii Financial Services Association

TESTIMONY OF MICHAEL TANOUE

COMMITTEE ON COMMERCE, CONSUMER PROTECTION, AND HEALTH
Senator Rosalyn H. Baker, Chair
Senator Stanley Chang, Vice Chair

COMMITTEE ON TECHNOLOGY
Senator Jarrett Keohokalole, Chair
Senator J. Kalani English, Vice Chair

Tuesday, March 17, 2020
9:00 a.m.

HB 2572, HD2

Chair Baker, Vice Chair Chang, and members of the Committee on Commerce, Consumer Protection, and Health, and Chair Keohokalole, Vice Chair English, and members of the Committee on Technology, my name is Michael Tanoue, counsel for the Hawaii Insurers Council. The Hawaii Insurers Council is a non-profit association of property and casualty insurance companies licensed to do business in Hawaii. Members companies underwrite approximately forty percent of all property and casualty insurance premiums in the state.

Hawaii Insurers Council **opposes** HB 2572, HD2. The property and casualty insurance industry is highly regulated, by state. In addition, the National Association of Insurance Commissioners (NAIC) regularly meet to confer, discuss, and develop model laws that are enacted across the nation to address issues that are universal, such as data security.

Currently, there are many specific state statutes that govern the way insurers treat personal information, data, and privacy including:

1. HRS Sec. 431:3A, Part I: general provisions;
2. HRS Sec. 431:3A, Part II: privacy and opt out notices for financial information;
3. HRS Sec. 431:3A, Part III: limits on disclosures of financial information;
4. HRS Sec. 431:3A, Part IV: exceptions to limits on disclosures of financial information;

5. HRS Sec. 487J-2: social security number protection;
6. HRS Sec. 487J-6: unlawful use of identification card or driver's license;
7. HRS Sec. 431:3-305: accounts; records;
8. HRS Sec. 431:9-229: records of adjuster or independent bill reviewer;
9. HRS Sec. 431:9A-123: records of insurance producer;
10. HRS Sec. 487R-2: destruction of personal information records;
11. HRS Sec. 431:3A-502: non-discrimination;
12. HRS Sec. 431:3A-203: information to be included in privacy notices;
13. HRS Sec. 431:3A-501: protection of Fair Credit Reporting Act; and
14. HRS Sec. 431:3A-503: violation shall be deemed an unfair method of competition or unfair or deceptive trade act or practice.

There are also Hawaii Supreme Court decisions that protect consumers' state constitutional right of privacy in health information:

1. Cohan v. Ayabe, 132 Hawaii 408, 322 P.3d 948 (2014)
2. Brende v. Hara, 113 Hawaii 424, 153 P.2d 1109 (2007)

Finally, the NAIC has developed a Data Security Model Law which we believe will be introduced for adoption in Hawaii as soon as in the 2021 Legislature. For these reasons, we believe the aforementioned bill is overly broad, premature, and if enacted, should exempt insurers licensed under Section 431:3A-102, Hawaii Revised Statutes.

Thank you for the opportunity to testify.



March 16, 2020

Senator Rosalyn H. Baker
Chair of the Committee on Commerce, Consumer Protection, and Health
Hawaii Senate
Hawaii State Capitol, Room 230
415 South Beretania Street
Honolulu, HI 96813

Senator Jarrett Keohokalole
Chair of the Committee on Technology
Hawaii Senate
Hawaii State Capitol, Room 203
415 South Beretania Street
Honolulu, HI 96813

RE: Testimony in Opposition to HI HB 2572, H.D. 2

Dear Chair Baker and Chair Keohokalole:

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies across the country including businesses in Hawaii, from small businesses to household brands, advertising agencies, and technology providers. Our combined membership includes more than 2,500 companies, is responsible for more than 85 percent of the U.S. advertising spend and drives more than 80 percent of our nation's digital advertising spend. We and the companies we represent strongly believe consumers deserve meaningful privacy protections supported by reasonable government policies.

While we fully support the legislature's intent to provide Hawaiians with strong privacy protections, we oppose HB 2572 in its current form. HB 2572 contains provisions that could harm consumers' ability to access products and services and exercise choice in the marketplace. The bill also contains particularly onerous terms surrounding digital data that could upend the Internet advertising ecosystem as we know it, disrupting consumers' online experience. Moreover, HB 2572 takes an approach that is highly inconsistent with other state privacy laws and privacy bills that are progressing through various state legislatures, while failing to develop a system that will work well for consumers or enhance a fair and competitive marketplace. In certain respects, the bill attempts to adopt definitions and structural elements of the California Consumer Privacy Act ("CCPA"). However, the CCPA is an incomplete statute, as the regulations implementing its terms have not yet been finalized. Furthermore, the CCPA contains various internal inconsistencies and ambiguities, and as such it should not be used as a basis for legislation in other states. For these reasons, we strongly oppose Hawaii's HB 2572.¹

I. The Data-Driven and Ad-Supported Online Ecosystem Benefits Consumers and Fuels Economic Growth

Today, the U.S. economy is increasingly fueled by the free flow of data. One driving force in this ecosystem is data-driven advertising. Advertising has helped power the growth of the Internet for decades by delivering innovative tools and services for consumers and businesses to connect and

¹ HB 2572, 30th Legislature, Reg. Sess. (Haw. 2020) (hereinafter "HB 2572").

communicate. Data-driven advertising supports and subsidizes the content and services consumers expect and rely on, including video, news, music, and more. Data-driven advertising allows consumers to access these resources at little or no cost to them, and it has created an environment where small publishers and start-up companies can enter the marketplace to compete against the Internet's largest players.

As a result of this advertising-based model, U.S. businesses of all sizes have been able to grow online and deliver widespread consumer and economic benefits. According to a March 2017 study entitled *Economic Value of the Advertising-Supported Internet Ecosystem*, which was conducted for the IAB by Harvard Business School Professor John Deighton, in 2016 the U.S. ad-supported Internet created 10.4 million jobs.² Calculating against those figures, the interactive marketing industry contributed \$1.121 trillion to the U.S. economy in 2016, doubling the 2012 figure and accounting for 6% of U.S. gross domestic product.³

Consumers, across income levels and geography, embrace the ad-supported Internet and use it to create value in all areas of life, whether through e-commerce, education, free access to valuable content, or the ability to create their own platforms to reach millions of other Internet users. Consumers are increasingly aware that the data collected about their interactions on the web, in mobile applications, and in-store are used to create an enhanced and tailored experience. Importantly, research demonstrates that consumers are generally not reluctant to participate online due to data-driven advertising and marketing practices. Indeed, as the Federal Trade Commission noted in its recent comments to the National Telecommunications and Information Administration, if a subscription-based model replaced the ad-based model, many consumers likely would not be able to afford access to, or would be reluctant to utilize, all of the information, products, and services they rely on today and that will become available in the future.⁴ It is in this spirit—preserving the ad supported digital and offline media marketplace while helping to design appropriate privacy safeguards—that we provide these comments.

II. The Bill's Definition of Personal Information for Breach Notification Purposes Extends Beyond Any State Law

HB 2572 would greatly expand the definition of “personal information” subject to the state's data breach notification law by including identifiers in its scope.⁵ Rendering such identifiers subject to the state's breach notification statute represents a massive expansion of breach notification requirements far beyond what any other state has done before. Even the CCPA does not include information used to identify individuals across technology platforms in its scope of information subject to the data breach enforcement provisions in the law.⁶ Expanding Hawaii's definition of “personal information” for data breach notification in this way would make Hawaii be out of step with other states and cause a vastly increased number of notices sent to consumers, thereby unnecessarily raising consumer alarm without providing any additional privacy protections.

The definition of “personal information” for the purposes of Hawaii's breach notification statute should be comprised of data elements that could enable identity theft if misappropriated. Identifiers across technologies do not pose the same risks to consumers as other data elements that should rightly be

² John Deighton, *Economic Value of the Advertising-Supported Internet Ecosystem* (2017), located at <https://www.iab.com/wp-content/uploads/2017/03/Economic-Value-Study-2017-FINAL2.pdf>.

³ *Id.*

⁴ Federal Trade Commission, *In re Developing the Administration's Approach to Consumer Privacy*, 15 (Nov. 13, 2018), located at https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf.

⁵ HB 2572, Part II, § 2.

⁶ Cal. Civ. Code § 1798.150(a)(1).

included in the scope of breach notification requirements. We therefore recommend that you not alter the definition of personal information for breach notification purposes.

III. The Bill Would Severely Impede Internet Commerce

The bill would also require opt-in consent for any sale of geolocation information and “internet browser information,” defined as “information from a person’s use of the internet,” including web browsing history, application usage history, origin and destination IP addresses, device identifiers, and the content of communications comprising Internet activity.⁷ This right to opt in to personal information sale is far different from other states’ approaches to personal information in the context of consumer privacy laws. If left uncorrected, HB 2752 would undermine the ad-supported Internet, crippling the online marketplace and resulting in a fractured experience for Hawaiian consumers.

Requiring opt-in consent for the sale of geolocation information and internet browser information would fundamentally change Hawaiians’ ability to access products and services they enjoy and expect through the Internet. Moreover, this approach is far out of step with other states’ consumer privacy proposals, such as the CCPA and others that impose an opt out regime to data sales rather than an opt in regime. HB 2572 defines “sale” broadly as “selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means,” geolocation information or internet browser information to another business or a third party for monetary or other valuable consideration.⁸ As a result, any transfer of such data is likely a “sale” under the bill, which provides no customary exemptions for service providers or other entities that businesses rely on for various processing activities, and which a consumer would reasonably expect to receive the information. Additionally, consumers would be inundated with requests for their consent to transfer internet browser information, thereby overwhelming them with a variety of notices and requests and causing significant consumer frustration.

Transfers of data over the Internet enable modern digital advertising, which subsidizes and supports the broader economy and helps to expose consumers to products, services, and offerings they want to receive. In a survey commissioned by the Digital Advertising Alliance, 90% of consumers stated that free content was important to the overall value of the Internet and 85% surveyed stated they prefer the existing ad-supported model, where most content is free, rather than a non-ad supported Internet where consumers must pay for most content.⁹ The survey also found that consumers value the ad-supported content and services at almost \$1,200 a year.¹⁰ The opt-in requirements of HB 2572 could destroy this model, which consumers have expressed that they value and would not want to see replaced. We therefore respectfully ask you to remove the opt in consent requirements for “sales” of geolocation information and internet browser information.

* * *

We and our members support Hawaii’s commitment to provide consumers with enhanced privacy protections. However, we believe HB 2572 takes an approach that will severely harm the online economy without providing helpful privacy protections for consumers. We therefore respectfully ask you to reconsider the bill and update it to remove the terms we discussed in this letter so Hawaiians can continue to receive products, services, and offerings they value and expect over the Internet.

⁷ HB 2572, Part III, § 4.

⁸ *Id.*

⁹ Zogby Analytics, Public Opinion Survey on Value of the Ad-Supported Internet (May 2016).

¹⁰ Digital Advertising Alliance, Zogby Poll: Americans Say Free, Ad-Supported Online Services Worth \$1,200/Year; 85% Prefer Ad-Supported Internet to Paid, PR Newswire (May 11, 2016).

Thank you in advance for consideration of this letter.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers
202-269-2359

Christopher Oswald
SVP, Government Relations
Association of National Advertisers
202-269-2359

David LeDuc
Vice President, Public Policy
Network Advertising Initiative
703-220-5943

Alison Pepper
Senior Vice President
American Association of Advertising Agencies, 4A's
202-355-4564

David Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau
202-800-0771

Clark Rector
Executive VP-Government Affairs
American Advertising Federation
202-898-0089

STATE PRIVACY AND SECURITY COALITION

March 16, 2020

Senator Rosalyn Baker
Chair, Senate Committee on Commerce,
Consumer Protection, and Health
Hawaii State Capitol, Room 230
Honolulu, HI 96813

Senator Jarrett Keohokalole
Chair, Senate Committee on Technology
Hawaii State Capitol, Room 203
Honolulu, HI 96813

Re: HB 2572 (Oppose)

The State Privacy & Security Coalition, a coalition of 30 leading telecommunications, technology, retail, payment card, online security, and automobile companies, as well as eight trade associations, writes to oppose HB 2572, which attempts to amend the state's data breach law, regulate geolocation specifically, and regulate internet browsing activity. HB 2572 contains outlier requirements that are overly broad and do not reflect mainstream privacy and data security protocols, and would have significant unintended consequences.

I. Data Breach Amendments

The primary principle of data breach notification laws is to provide the affected residents with clear, accurate, and comprehensive information about breaches that pose risk to them. In this area of law, uniformity benefits consumers. The greater the uniformity, and the clearer the definition of data elements that trigger a notice requirement, the more efficiently notices can be provided to the affected individuals, regardless of state lines.

HB 2572's proposed definition of "Identifier" would make Hawaii a problematic outlier in the data breach statute ecosystem. It is unclear, overly broad, and there is nothing like it in any other state statute. It would create consumer confusion because instead of defining identifier as an individual's first initial and last name, or first name and last name, it defines the term as "a common piece of information related specifically to an individual...to identify that individual across technology platforms." Most fundamentally, this type of information, a somewhat amorphous range of data elements, such as advertising cookie ID numbers, internet protocol addresses, and mobile advertising identification numbers *cannot be used* in combination with a "specified data element" by fraudsters to commit identity theft or fraud. Instead, the individual's name is required. It therefore would be counterproductive to replace the term "identifier" for "name" in current law.

Additionally, the "Specified data element" definition contains several overbroad provisions. First, unlike all other state breach notice laws, paragraph (1) would require notice of breaches of the last 4 digits or more of social security numbers. The last 4 digits of an SSN is the most

STATE PRIVACY AND SECURITY COALITION

common way to redact SSNs, and in this form, they cannot be used without the rest of the SSN to commit identity theft or fraud. What is more, redaction of SSNs and other sensitive data elements is a good security practice. Yet requiring breach notice of redacted SSNs would eliminate the incentive for businesses to protect the data this way.

Second, nearly every other state combines the elements in (4) and (5) (financial account information and information that allows access to an account). This is because on their own, each data element is not enough to cause a Hawaii resident harm. A credit card number without the security code, or an email account without the password, presents limited danger to the consumer and would result in increased, and meaningless, consumer notifications where no threat of identity theft exists.

What is more, paragraph (5) as drafted reaches *any* access code or password to *any* individual account. It would cover passwords for a host of accounts that create no risk to individuals, if breached – for example, passwords for online news sites, streaming video accounts, dry cleaning, supermarket and other retail accounts. The passwords to these accounts create minimal risk of identity theft or fraud. No state requires notice for breaches of these passwords, because they pose no risk, and Hawaii should not do so either.

II. Geolocation Information & Internet Browser Information

The bill also attempts to restrict the use of both geolocation information and internet browser activity in ways that ignore the realities of the modern online ecosystem. The Twenty-First Century Privacy Law Task Force was responsible for looking at public policy considerations of privacy legislation and parts of this legislation, including internet browser information, was not part of the Task Force's recommendations of information to regulate. Since there was little input by the entities this bill seeks to regulate during that process, we ask that that this bill be tabled and that the task force hold meetings on this issue and study it further before proceeding with broad regulation of this area.

a. Geolocation Data

Section 4 is broad and ambiguous in a way that is likely to have significant unintended consequences. The Federal Trade Commission's (FTC) 2012 privacy framework notes that precise geolocation is sensitive information for which an entity should receive consent before using, and we do not oppose such a requirement. However, any bill attempting to regulate this should be carefully considered.

HB 2572 includes a very broad definition of "sell" that includes any disclosure in exchange for anything of value. The bill requires opt-in consent for all these disclosures – whereas even the California Consumer Privacy Act (CCPA) requires only an opt-out and contains many exceptions not present in HB 2572. By way of example, there is no fraud exemption, so that fraudsters could refuse to be tracked and avoid triggering red flags in systems that use location as an element that subjects suspicious transactions to closer inspection and identify patterns that

STATE PRIVACY AND SECURITY COALITION

help to prevent future unlawful activities. Likewise, services that allow parents to track the movement of their children's phones would likely require opt-in consent of the children.

These problems would ensue due to the use of the CCPA's definition of "sale" – a definition which produces most of CCPA's unintended consequences. Using this definition here with an opt-consent requirement would cause more extreme unintended consequences. For example, if a consumer requests a transaction that involves the disclosure of location information from a business to its service provider, must the consumer provide express consent to do so? What if the consumer requests such a transaction but does not provide the consent necessary to complete the transaction? The same is true of a host of other location-based services that do not actually involve "sale" of location data, but where there is some form of compensation offered in connection with location data that is used to deliver a service that users seek or expect.

The definition of "geolocation information" is so broad as to include every photograph or video that is captured by a phone and transferred by a photo application to a cloud storage company. It could also include any information that contains a consumer's zip code, which would provide some broad sense of a consumer's location; or information that contains a customer's purchase history but does not include geolocation information. These types of unintended consequences should be avoided.

Of course, Hawaii is a unique and treasured tourist destination. The Hawaii Tourism Authority estimated that in 2017, nearly 10 million tourists visited. If every tourist took even 5 photos, that would be 50 million photos generated. Subjecting each one of these to enforcement as a result of, for example, a consumer transferring a photograph from a consumer's email account to his or her social media account is likely not what the legislature intends to regulate, but by applying the CCPA's definition of "sale," that is exactly what would occur.

In short, this section raises far-reaching implications, and should be removed from the bill this year, be studied appropriately and refined before being considered next year.

b. Internet Browser Information

The second part of section 4 creates similar issues. First, it goes significantly beyond the Obama Administration FTC Privacy Framework, which does not consider browsing history as sensitive information. It would have significant unintended consequences because types of this information are frequently transferred to keep the provision of services free, as well as to detect suspicious and fraudulent activity that harms individuals conducting legitimate online activity.

Similar to the problems created by using the CCPA definition of "sale" with geolocation information, using the definition of "sale" in the context of internet browser information fails to account for the modern online ecosystem. The bill would impose unreasonable and unwarranted obligations before an internet service provider or any other entity could perform functions that consumers expect.

STATE PRIVACY AND SECURITY COALITION

If consumers do not opt in to uses of data that permit companies to develop new products and services, or to sharing of cybersecurity threat information, both businesses and consumers will suffer. Similarly, much of the free news and content that is available online is supported by advertising, which takes place through the exchange of pseudonymous identifiers. This presents little risk to individuals, who may already opt out of the use of their data for most advertising purposes.¹ Requiring consumers to opt in to these low-risk uses of information that are central to the delivery of online services is likely to adversely affect availability of these free or low cost services that consumers want and enjoy.

In conclusion, HB 2572 contains confusing requirements in much of the bill that are overbroad and do not account for the modern online ecosystem. We would be willing to work with your committees on a better alternative that achieves the same comprehensive goals, but is much simpler and provides clearer and more meaningful consumer benefits.

Respectfully submitted,



Andrew Kingman
General Counsel
State Privacy and Security Coalition

¹ See, e.g., Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, 40-44 (2012); CAN-SPAM CITE; Self-Regulatory Principles for Online Behavioral Advertising (July 2009), available at: <http://www.aboutads.info/resource/download/seven-principles-07-01-09.pdf>; Network Advertising Initiative Code of Conduct (2018), available at: http://www.networkadvertising.org/sites/default/files/nai_code2018.pdf.



Tammy Cota, Executive Director
1 Blanchard Court, Suite 101
Montpelier, VT 05602
802-279-3534
tammy@theinternetcoalition.com
www.theinternetcoalition.com

March 17, 2020

Honorable Rosalyn Baker, Chair
Senate Commerce, Consumer Protection and Health Committee

Honorable Jarrett Keohokalole, Chair
Senate Technology Committee

415 South Beretania Street
Honolulu, HI 96813

RE: Opposition to HB 2572, Relating to Privacy

Dear Senator Baker and Senator Keohokalole:

I am the executive director of the Internet Coalition (IC), a national trade association that represents members in state public policy discussions. The IC also serves as an informational resource, striving to protect and foster the Internet economy and the benefits it provides consumers.

The IC wants to express **opposition to HB 2572**. While protecting customer privacy and adhering to strong consumer privacy protections are an essential element in building and maintaining consumer trust, IC urges you not to advance this bill as it would cause companies to issue expensive data breach notices to consumers, potentially causing widespread panic and substantial reputational losses for breaches of low-risk data; would disrupt users' online experiences and unnecessarily burden industry.

Part II of the bill proposes to expand upon Hawaii's data security breach notification law by adding identifiers to personal information that would require consumer notice. The proposed changes would mean that companies would have to provide notices when non-identifying information has been acquired and when data combinations were accessed but did not actually provide a criminal with the ability to access a user account. For example, notices would be required if a person's phone number and account password were accessed, despite the lack of a person's name or without enough information to illegally access an account. No other state data breach law requires notices to consumers unless data combinations obtained would identify an individual.

Part III of the bill proposes to require explicit consent to share or sell a person's geolocation or internet browser information. The definition of "sale" would cover disclosure of information in any form, and not just for monetary consideration. Prior "consent" could be revoked at any time. "Internet browser information" is defined broadly to apply to any data related to internet use, most of which is not considered sensitive or personal information. It is unlikely intentional, but obtaining the numerous consents required would cause delays, disruptions or even prevent online companies from completing traditional, routine online transactions which a customer has

requested. Shoppers that are suddenly subjected to numerous opt in requests for low risk uses of information will be confused, frustrated and turned off when their favorite sites and services are no longer convenient or enjoyable.

Part VI of the bill references providers of electronic communication services and remote computing services, while Part V gives such providers immunity from liability. However, there is no exclusion given for providers of Internet communication services which are often misused by perpetrators to cause display of illegal content. *See* 47 U.S.C. §§ 230(f)(2) and (3), a Federal law that recognized that companies that host content from hundreds of thousands or millions of third parties cannot reasonably be expected to police them – and therefore should not be liable for third-party content, *see* 47 U.S.C. § 230(c). The lack of this exclusion in this bill may lead prosecutors and plaintiff's lawyers to mistakenly think that such providers could be held liable for end-user third-party postings.

The bill's provisions would be enforceable under Hawaii's Consumer Protection statute, which allows for class action enforcement. Class action attorneys lack the expertise possessed by the Attorney General's Office and are motivated by profit, not consumer protection. Particularly since this legislation proposes mandates not found in other state laws, we are deeply concerned that compliance guidance will end up being resolved through needless, costly and unnecessary litigation that could force companies into bankruptcy.

For the reasons stated above, we urge you to **REJECT HB 2572** and avoid unnecessarily alarming consumers of low-risk data breaches, disrupting user's online experiences and unnecessarily burdening industry. IC stands ready to help craft a forward-thinking privacy law that ensures consumer privacy rights while remaining flexible enough to promote industry innovation and growth.

Please let me know if you would like more information or have questions.

Sincerely,



Tammy Cota

cc: Senate Commerce, Consumer Protection and Health Committee members
Senate Technology Committee members



SanHi

GOVERNMENT STRATEGIES

A LIMITED LIABILITY LAW PARTNERSHIP

DATE: March 16, 2020

TO: Senator Rosalyn Baker
Chair, Committee on Commerce, Consumer Protection & Health

Senator Jarrett Keohokalole
Chair, Committee on Technology
Submitted Via Capitol Website

FROM: Mihoko Ito

RE: **H.B. 2572, H.D. 2 - Relating to Privacy**
Hearing Date: Wednesday, March 17, 2020 at 9:00 a.m.
Conference Room: 229

Dear Chair Baker, Chair Keohokalole and Members of the Joint Committees:

We offer this testimony on behalf of the Consumer Data Industry Association (CDIA). Founded in 1906, CDIA is the international trade association that represents more than 100 data companies. CDIA members represent the nation's leading institutions in credit reporting, mortgage reporting, fraud prevention, risk management, employment screening, tenant screening and collection services.

CDIA **submits comments** on H.B. 2572, H.D. 2, Relating to Privacy. As currently drafted, Part 3, Section 4 of the bill requires opt in consents for collecting data relating to geolocation and internet browser history.

CDIA opposes the current language in these sections because these proposed requirements would negatively impact and in some cases prevent important fraud prevention activities of CDIA's members.

With respect to the geolocation requirements, using geolocation in the application of fraud detection has been proven to increase detection rates and reduce false positives. Geolocation technology can be used to automatically block suspect traffic, request verification (via email or SMS), or flag suspect activity for further internal review. Geolocation can be a key marker to identify suspect proxies, VPNs, other at-risk devices used by would-be identity thieves. In addition, in the context of fraud prevention, this digital element can help businesses and the government agencies who partner with private vendors for fraud detection support to identify and respond to greater numbers of suspicious online connections.

Similarly, with respect to internet browser history, if opt-in consents are required when fraud prevention questions or information is sought by consumer data companies, fraudsters would be in control of opting out of capturing data needed to legitimately verify identity. This would result in unintended consequences, by allowing fraudsters the option

to opt out of providing information, and decreasing the ability to protect the identity verification process.

For the above reasons, we would respectfully request that if the Committees are inclined to move this measure forward, that the following amendment be incorporated for the provisions relating to geolocation (starting at page 8, line 10) and internet browser histories (starting at page 10, line 7) to exempt fraud prevention activities in both sections as follows:

This section shall not apply to any activity involving the collection, maintenance, disclosure, sale, communication, or use of internet browser information to protect against, prevent, detect, investigate, verify or respond to security incidents, identity theft, identity, fraud, harassment, unauthorized transactions or claims, or to confirm or reconcile transactions, or to prevent malicious or deceptive acts, or any illegal activity.

Thank you very much for the opportunity to testify on this measure.



Charter Communications
[REVISED] Testimony of Myoung Oh, Director of Government Affairs

COMMITTEE ON COMMERCE, CONSUMER PROTECTION, AND HEALTH

COMMITTEE ON TECHNOLOGY

Hawai'i State Capitol, Conference Room 229
Tuesday, March 17, 2020
9:00 AM

CONCERNS ON H.B. 2572, H.D.2 , RELATING TO PRIVACY

Chair Baker, Chair Keohokalole, Vice-Chair Chang, Vice-Chair English and Members of the Joint Committees.

Charter Communications, Inc. ("Charter") is pleased to have this opportunity to provide its views on H.B. 2572, H.D.2. As explained below, Charter supports Hawai'i's efforts to protect the privacy of consumer personal data and give consumers meaningful control of their personal data. Charter looks forward to continuing to work with the Committee on Commerce, Consumer Protection and Health, the Committee on Technology, and other stakeholders to achieve those goals. While we acknowledge the changes to the bill since its introduction and support the concepts behind the legislation, we oppose enactment of the bill in its current form until certain clarifications are made to address several unintended consequences.

As the largest broadband provider in Hawai'i with services available to over 400,000 homes and businesses in all 4 counties, including Molokai and Lanai, Charter Communications is committed to providing Hawai'i consumers with superior products and services. As a result of significant network

investments, Charter's base broadband speed is 200/10Mbps, and we now offer Spectrum Internet Gig (with download speeds of 940 Mbps) across most of Hawai'i. Charter continues to significantly invest in and provide infrastructure improvements, unleashing the power of an advanced, two-way, fully interactive fiber network. By moving to an all-digital network, today's Spectrum customers enjoy more HD channels, more On Demand offerings, more video choices than ever before, and the fastest internet speeds and the most consistent performance available. Charter offers these services without data caps, modem fees, annual contracts, or early termination fees.

An increasingly important aspect of ensuring that consumers continue to utilize all the services the internet has to offer is making sure they are confident that their personal information is protected. Charter enthusiastically supports such protections, and has taken an active role here and in other forums to promote potential approaches to address the complex issues that impact consumers' online privacy. As Charter has expressed in testimony before the United States Congress and in state houses across the country, an effective privacy framework must be based primarily on five principles.

The first principle is control. Consumers should be empowered to have meaningful choice regarding the collection and use of their data. Any legal framework that is ultimately adopted should ensure consumer consent is purposeful, clear, and meaningful. Additionally, consent should be renewed with reasonable frequency, and any use of personal data should be reasonably limited to what the consumer understood at the time consent was provided. We recognize that there are several policy options as to how to provide consumers with control of their information, and we are willing to work with stakeholders to find practical and impactful solutions.

The second principle is transparency. Consumers should be given the information they need to provide informed consent. Explanations about how companies collect, use and maintain consumers' data should be clear, concise, easy-to-understand, and readily available.

The third principle is parity. Consumers are best served by a uniform framework that is applied consistently across the entire internet ecosystem, not based on who is collecting it or what type of service is being offered. Consumers' data should be protected equally whether they are using an ISP, a search engine, an e-commerce site, a streaming service, a social network, or a mobile carrier or device.

The fourth principle is uniformity. We believe that for online consumer protections to be effective there should be a single national standard. A patchwork of state laws would be confusing for consumers, difficult for businesses to implement, and hinder continued innovation. However, we realize that in the absence of a uniform, federal solution, some states may consider acting on their own. In doing so, it will be critical that the states understand what each of the others is doing so as to avoid an inconsistent or worse, contradictory, set of online protections.

The final principle is security. We believe privacy is security and security is privacy. Strong data security practices should include administrative, technical, and physical safeguards to protect against unauthorized access to personal data, and ensure that these safeguards keep pace with technological development.

CONCERNS WITH H.B. 2572, H.D.2

In our testimony earlier this year before the Committee on Judiciary and Committee on Consumer Protection, Commerce, and Health, we highlighted our concerns with substantial portions of H.B. 2572, H.D.2, which were derived from an outdated form of the California Consumer Privacy Act of 2018 (the “CCPA”). We appreciate the changes made so far to H.B. 2572, H.D.2 that remove these provisions.

However, H.B. 2572, H.D.2 still contains several problematic provisions, specifically those related to “geolocation information” and “internet browser information.” Both of these provisions continue to rely on an outdated and partial definition of “sale” taken from an earlier, and now superseded, version of the CCPA. For example, H.B. 2572 fails to include exceptions for fraud prevention, cybersecurity, internal uses, or deidentified or aggregated information.

Part III of H.B. 2572, H.D.2 also suffers from several additional shortcomings. Part III of H.B. 2572, H.D.2 applies its consent rights to “subscribers,” “users,” and “primary users,” but does not clearly distinguish between those terms or even provide a definition for “primary user.” Likewise, the bill mandates that businesses obtain “explicit consent” from consumers, but only provides a definition for “consent,” leaving open the question of whether “explicit consent” is something different. More troubling is that Part III of H.B. 2572, H.D.2 represents legislation for which the Twenty-first Century Privacy Law Task Force, “did not review any specific proposed legislation on the subject.” Part III of H.B. 2572, H.D.2 therefore has not been subject to the type of review and consideration that makes for sound, well-reasoned privacy legislation.

These are important issues, and consumers deserve to have the protections envisioned by the task force and the authors of H.B. 2572, H.D.2. But we encourage the legislature to take the additional time necessary to ensure that the provisions of H.B. 2572, H.D.2 are clear to businesses and consumers, and provide sufficient and sustainable privacy protections.

CONCLUSION

Charter is committed to ensuring that consumer information is protected across the internet ecosystem. That is why, two years ago, our CEO broke new ground by calling for the enactment of federal legislation mandating that all companies receive affirmative, opt-in consent before collecting or sharing their customers' data. And since that time, Charter representatives have appeared voluntarily and on numerous occasions before lawmakers and policymakers—including Congress and the Federal Trade Commission—to support such a federal privacy law.

Charter looks forward to continuing to work with Members of these Committees, industry partners, consumer groups, and other stakeholders in this process to address the privacy of local residents holistically, sensibly, and effectively through more deliberate legislation.

Thank you again for the opportunity for Charter to present its views.



SanHi

GOVERNMENT STRATEGIES

A LIMITED LIABILITY LAW PARTNERSHIP

DATE: March 16, 2020

TO: Senator Rosalyn Baker
Chair, Committee on Commerce, Consumer Protection & Health

Senator Jarrett Keohokolole
Chair, Committee on Technology
Submitted Via Capitol Website

FROM: Mihoko Ito

RE: **H.B. 2572, HD1 - Relating to Privacy**
Hearing Date: Thursday, February 20, 2020 at 10:00 a.m.
Conference Room: 229

Dear Chair Baker, Chair Keohokolole and Members of the Joint Committees:

We offer this testimony on behalf of the Consumer Data Industry Association (CDIA). Founded in 1906, CDIA is the international trade association that represents more than 100 data companies. CDIA members represent the nation's leading institutions in credit reporting, mortgage reporting, fraud prevention, risk management, employment screening, tenant screening and collection services.

CDIA **submits comments** on H.B. 2572, HD1 Relating to Privacy. As currently drafted, Part 3, Section 4 of the bill requires opt in consents for collecting data relating to geolocation and internet browser history.

CDIA opposes the current language in these sections because these proposed requirements would negatively impact and in some cases prevent important fraud prevention activities of CDIA's members.

With respect to the geolocation requirements, using geolocation in the application of fraud detection has been proven to increase detection rates and reduce false positives. Geolocation technology can be used to automatically block suspect traffic, request verification (via email or SMS), or flag suspect activity for further internal review. Geolocation can be a key marker to identify suspect proxies, VPNs, other at-risk devices used by would-be identity thieves. In addition, in the context of fraud prevention, this digital element can help businesses and the government agencies who partner with private vendors for fraud detection support to identify and respond to greater numbers of suspicious online connections.

Similarly, with respect to internet browser history, if opt-in consents are required when fraud prevention questions or information is sought by consumer data companies, fraudsters would be in control of opting out of capturing data needed to legitimately verify identity. This would result in unintended consequences, by allowing fraudsters the option

to opt out of providing information, and decreasing the ability to protect the identity verification process.

For the above reasons, we would respectfully request that if the Committees are inclined to move this measure forward, that the following amendment be incorporated for both the provisions relating to geolocation (starting at page 8, line 10) and internet browser histories (starting at page 10, line 7) to exempt fraud prevention activities in these sections as follows:

This section shall not apply to any activity involving the collection, maintenance, disclosure, sale, communication, or use of internet browser information to protect against, prevent, detect, investigate, verify or respond to security incidents, identity theft, identity, fraud, harassment, unauthorized transactions or claims, or to confirm or reconcile transactions, or to prevent malicious or deceptive acts, or any illegal activity.

Thank you very much for the opportunity to testify on this measure.



IATSE Mixed Local 665 HAWAII'S TECHNICIANS

LATE

for
FILM, TELEVISION, STAGE AND PROJECTION
Since 1937

INTERNATIONAL ALLIANCE OF THEATRICAL STAGE EMPLOYEES, MOVING PICTURE TECHNICIANS, ARTISTS AND ALLIED CRAFTS
OF THE UNITED STATES, ITS TERRITORIES AND CANADA, AFL-CIO, CLC

Date: March 16, 2020

To: The Honorable Senator Rosalyn H. Baker, Chair, CPH
The Honorable Senator Stanley Chang, Vice Chair, CPH
Members of the Senate Committee on Commerce, Consumer Protection and Health

The Honorable Senator Jarrett Keohokalole, Chair, TEC
The Honorable Senator J. Kalani English, Vice Chair
Members of the Senate Committee on Technology

Re: HB 2572 HD 2: RELATING TO PRIVACY

HEARING DATE/TIME: TUESDAY, MARCH 17TH, 2020, AT 9:00 AM

CONFERENCE ROOM: Room: 229, Hawai'i State Capitol

Aloha, Chairs Baker and Keohokalole, Vice Chairs Chang and English, and Members of the Committees:

Mahalo for hearing this very important bill. We **SUPPORT** SECTION V of HB 2572, HD 2 found on Page 20 of the bill, and request your support in making it a Class C Felony to intentionally create and distribute an image or video of a known person over a nude image of an unknown person without their knowledge or consent, otherwise known as deepfake pornography.

The sophistication of Computer-Generated Imagery (CGI) makes it nearly impossible to tell if an image or video is real or fake. There are thousands of these damaging images on the Internet, and many people's lives and careers have been maliciously harmed by these non-consensual, fake images.

Over 1,000 SAG-AFTRA members have been victims of deepfake pornography, and it is being used to harass college student and ex-girlfriends.

This privacy protection is a basic human right to be free from abuse and harassment and will punish and deter those who intentionally use deepfake pornography to harm innocent people. Mahalo for your support of this important bill to take back our right to privacy.

Respectfully,

Irish Barber
Business Representative



Testimony of
GERARD KEEGAN
CTIA

In Opposition to Hawaii House Bill 2572 HD2

Before the
Hawaii Senate Committee on Commerce, Consumer Protection, & Health and Committee on Technology

March 17, 2020

Chairs, Vice-Chairs, and committee members, on behalf of CTIA®, the trade association for the wireless communications industry, I submit this testimony in opposition to House Bill 2572 HD2. This bill is overly broad and would have serious unintended consequences.

Section 4 dealing with internet browser information imposes unreasonable restrictions on internet service providers and other internet companies that would negatively affect services that consumers have come to expect. The opt-in provisions in the bill may jeopardize the availability of consumer data for cybersecurity and fraud prevention purposes. This language also threatens the quality of free or low-cost goods and services, which rely on the use of personal data that is subject to safeguards, such as pseudonymization. Online news and other content are often provided to consumers free of charge because they are supported by advertising in exchange for pseudonymous identifiers. Having consumers opt-in for use of this low risk information could negatively impact the provision of low cost or free products and services. Moreover, the opt-in provision could inhibit providing new and innovative services to Hawaii consumers.

The Federal Trade Commission's privacy framework considers precise geolocation information as sensitive information. CTIA supports the FTC framework but has concerns with the geolocation section of HB 2572 HD2. For example, there is no fraud exception, so fraudsters could use the bill's provisions to avoid



identifying fraudulent activity. Additionally, these provisions would require children's opt-in consent before their parents or guardians can initiate a tracking service or application. The definition of "geolocation information" is also overly broad and will introduce a host of unintended consequences. For example, a consumer's zip code would fall under the definition of geolocation information, which is not the type of information that CTIA thinks the legislature intends to identify as geolocation information.

In closing, sweeping state legislation like HB 2572 HD2 could hamper the provision of internet service in Hawaii, prevent providing new and innovative products and services, and lead to increase compliance costs – all to the detriment of consumers. CTIA would recommend that these issues be more comprehensively studied to ensure that unintended consequences are mitigated. Accordingly, CTIA respectfully requests that you not move this legislation. Thank you for your consideration.

HB-2572-HD-2

Submitted on: 3/16/2020 8:11:39 AM

Testimony for CPH on 3/17/2020 9:00:00 AM

Submitted By	Organization	Testifier Position	Present at Hearing
Rayne	Individual	Support	No

Comments:

HB-2572-HD-2

Submitted on: 3/14/2020 12:13:15 PM

Testimony for CPH on 3/17/2020 9:00:00 AM

Submitted By	Organization	Testifier Position	Present at Hearing
Leanne N. Teves	Individual	Support	No

Comments:

HB2572 HD1 Relating to RELATING TO PRIVAC

Aloha

Commerce, Consumer Protection and Health Committee

Senator Rosalyn H. Baker, Chair

Senator Stanley Chang, Vice Chair and members

Committee on Technology

Senator Jarrett Keohokalole, Chair

Senator J. Kalani English, Vice Chair and members

My name is Leanne Natsuyo Teves and I support making the creation and distribution of deep fake pornography a felony (section V). I would like to thank the members of the Legislature for addressing this important issue of unlawful use of images violating privacy. The protection with this measure will allow the acting community as well as all citizens in our great state to be free from abuse and harassment.

Thank you for your time in reviewing my testimony.

DAVID C. FARMER

ATTORNEY AT LAW

225 Queen Street
Suite 15A
Honolulu, Hawai'i 96813

A LIMITED LIABILITY LAW COMPANY LLLC

Tele: (808) 888-3138
Fax: 1 (866) 559-2922
email: farmer6348@twc.com

March 15, 2020

THE SENATE
THE THIRTIETH LEGISLATURE
REGULAR SESSION OF 2020

COMMITTEE ON COMMERCE,
CONSUMER PROTECTION, AND HEALTH
Senator Rosalyn H. Baker, Chair
Senator Stanley Chang, Vice Chair

COMMITTEE ON TECHNOLOGY
Senator Jarrett Keohokalole, Chair
Senator J. Kalani English, Vice Chair

Hawai'i State Capitol
415 South Beretania Street
Conference Room 229

RE: HB 2572, HD2; (HSCR795-20): RELATING TO PRIVACY.
HEARING: Tuesday, March 17, 2020; 9:00 AM

Aloha Senators Baker, Chang, Keohokalole, and English; Members of the Committees on Commerce, Consumer Protection, and Health and on Technology:

My name is David C. Farmer. I am an attorney in private practice since 1985, a member of Screen Actors Guild-American Federation of Television and Radio Artists ("SAG-AFTRA"), Hawai'i Local since 1987, and a board member and current President of our Local since 2012. I rise as a private citizen in support of HB 2572, HD2; (HSCR795-20), making the creation and distribution of deepfake pornography a felony.

We sincerely appreciate the opportunity you and the Legislature have provided for addressing the important issues raised in this proposed legislation, especially Part V of HB 2572, HD2 that makes creating and distributing deepfake pornography a felony.

Not only an issue of great importance to our members, it is of importance to all our citizens as potential targets for this insidious evil that is sadly all-too common on the Internet. In addition to being used to harass college students and ex-girlfriends, deepfake pornography has harmed our SAG-AFTRA sisters and brothers, Also noting that deepfake pornography has been made of over 1,000 SAG-AFTRA members, including such prominent members as Emma Watson and Scarlett Johansson. In short, it can seriously harm you, your family, or anyone.

As you may know, deepfake pornography prominently surfaced on the Internet in 2017, particularly on Reddit. The first one that captured attention was the Daisy Ridley deepfake, which was featured in several articles. Other prominent pornographic deepfakes were of various other celebrities.

In December 2017, Samantha Cole published an article about deepfakes in *Vice* that drew the first mainstream attention to deepfakes being shared in online communities. Six weeks later, Cole wrote in a follow-up article about the large increase in AI-assisted fake pornography. Since 2017, she has published a series of articles covering news surrounding deepfake pornography.

Since then, multiple social media outlets have banned or made efforts to restrict deepfake pornography. Most notably, the r/deepfakes subreddit on Reddit was banned on February 7, 2018, due to the policy violation of “involuntary pornography.” In the same month, representatives from Twitter stated that they would suspend accounts suspected of posting non-consensual deepfake content.

Scarlett Johansson, a frequent subject of deepfake porn, spoke publicly about the subject to *The Washington Post* in December 2018. In a prepared statement, she expressed that despite concerns, she would not attempt to remove any of her deepfakes, due to her belief that they do not affect her public image and that differing laws across countries and the nature of internet culture make any attempt to remove the deepfakes “a lost cause.” While celebrities like herself are protected by their fame, however, she believes that deepfakes pose a grave threat to women of lesser prominence who could have their reputations damaged by depiction in involuntary deepfake pornography or revenge porn.

In June 2019, a downloadable Windows and Linux application called DeepNude was released that used neural networks, specifically generative adversarial networks, to remove clothing from images of women. The app had both a paid and unpaid version, the paid version costing \$50. On June 27, the creators removed the application and refunded consumers.

The bottom line is simply that a civilized society must provide this privacy kind of protection as a basic human right to be free from abuse and harassment. With the passage of HB 2572, HD2, Hawai`i will once again be a leader in the forefront of insuring safety and protection for all its citizens.

I urge your Committees to support this legislation and enact it this Session. Mahalo for your time and consideration.

In Solidarity and Looking Forward,

A handwritten signature in black ink, appearing to read "David C. Farmer". The signature is fluid and cursive, with the first name "David" being more prominent.

David C. Farmer

President
SAG-AFTRA Hawai`i Local

201 Merchant Street, Suite 2301
Honolulu, HI 96813

225 Queen Street, Ste. 15A
Honolulu, HI 96813

Tel: (808) 888-3138
Cell: (808) 222-3133

Aloha!

Thank you for addressing this important issue.

I am supporting SECTION VI of [HB2572 HD2](#) found on page 58.

I am supporting making the creation and distribution of deepfake pornography a felony. Many actors have had deepfakes make their lives miserable.

This privacy protection is a basic human right to be free from abuse and harassment.

Mahalo,

Jean Simon
4944 Kilauea Ave Apt 2
Honolulu, HI 96816

HB-2572-HD-2

Submitted on: 3/13/2020 10:38:37 PM

Testimony for CPH on 3/17/2020 9:00:00 AM

Submitted By	Organization	Testifier Position	Present at Hearing
Jalem Correia	Testifying for SAG-AFTRA	Support	No

Comments:

HB-2572-HD-2

Submitted on: 3/12/2020 9:50:36 PM

Testimony for CPH on 3/17/2020 9:00:00 AM

Submitted By	Organization	Testifier Position	Present at Hearing
Naomi Melamed	Individual	Support	No

Comments: